UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

KAUSHIK MAHIDA, Individually, and on Behalf of All Others Similarly Situated, Plaintiff, v. ILLINOIS GASTROENTEROLOGY GROUP, PLLC, Defendant.	)	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kaushik Mahida ("Plaintiff"), through his undersigned counsel, brings this action against Illinois Gastroenterology Group, PPC. ("IGG" or "Defendant") pursuant to the investigation of his attorneys, personal knowledge as to himself and his own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. Illinois Gastroenterology Group is a regional physicians' group, which was formed in 2010 from the merger of three different Illinois gastroenterology practices.

2. On or about April 23, 2022, IGG announced publicly that on October 22, 2021, it had been the recipient of a hack and exfiltration of sensitive personal information ("SPI") involving manyof its patients (the "Data Breach"). As of this writing, IGG has not identified the total number of affected individuals in the Data Breach.

3. IGG reported that this SPI included names, addresses, dates of birth, Social Security numbers, driver's license numbers, passport numbers, financial account information, payment card information, employer-assigned identification numbers, medical information, and biometric data.[1]

4. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. Additionally, on information and belief, the "financial information" referred to includes bank account and routing numbers for patient bank accounts, allowing criminals to make fraudulent withdrawals of money from those accounts.

6. The information stolen in cyber-attacks allows the modern thief to assume victims' identitie when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

7. Plaintiff's and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

8. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

---

[1] https://www.illinoisgastro.com/articles/notice-of-security-incident (last accessed April 30, 2022)

9. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under California data privacy laws; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant's principal places of business are located within this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

14. Plaintiff Kaushik Mahida is a natural person residing in Irvine, California. Plaintiff Mahida was a patient of IGG in 2018, at which time Defendant collected his SPI. On or about April 28, 2022, Plaintiff Mahida was informed via letter dated April 23, 2022 that he had been a victim of the Data Breach.

15. Defendant Illinois Gastroenterology Group, PLLC is a for-profit Illinois corporation with its principal place of business at 20 Tower Court, Gurnee, Illinois.

FACTUAL ALLEGATIONS

16. Defendant is a physicians' group with affiliated offices located in Northern and Central Illinois. Defendant sees at least thousands of patients per year at its various offices.

17. In the ordinary course of doing business with Defendant, patients and prospective patients are required to provide Defendant with SPI such as:

a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, security codes, and signature;

c. Demographic information, such as age, gender, and date of birth;

d. Payment information, such as credit card, debit card, and/or bank account number; and

e. Medical history as self-reported by patients, or medical history as transmitted from other healthcare providers;

f. Biometric data, as stated by Defendant in its Notice of Security Incident.

18. Defendant also automatically collects the following SPI from its patients, including medical and diagnosis history from its own physicians; treatment information; and prescription information, among other types of information.

19. Defendant prominently represents on its website: "Your privacy is important to us."[2]

20. Defendant also represents in its privacy policy that "Other uses and disclosures of your health information not covered by this Notice or the laws that apply to us will be made only with your authorization. If you authorize us to use or disclose your health information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information as specified by the revoked authorization, except to the extent that we have taken action in reliance on your previous authorization.."[3]

21. Defendant's Data Breach was not enumerated on its website or privacy policy as a basis for its disclosure of SPI.

22. On or about April 23, 2022, Defendant announced publicly that on October 22, 2021, it became aware of unusual activity within its network. Defendant further stated that on November 18, 2021 it determined that a hack and exfiltration of sensitive personal information involving its patients occurred.[4]

---

[2] https://www.illinoisgastro.com/patient-resources/patient-privacy-information (last accessed April 30, 2022)
[3] https://www.illinoisgastro.com/uploads/Notice_of_Privacy_Practices-3-13_2.pdf (last accessed April 30, 2022)
[4] https://www.illinoisgastro.com/articles/notice-of-security-incident (last accessed April 30, 2022)

23. Of concern, while Defendant became aware of the Data Breach no later than November 18, 2021, it took more than five months for Defendant to notify patients and the media of the breach.

24. While the Data Breach was reported in at least one trade journal at the time, there appears to have been no wide-scale press release as local press, such as WTTW, WBEZ, and the Chicago Tribune have not reported it as of this writing.

25. As a result, Plaintiff's and class members' SPI was in the hands of hackers for approximately six months before Defendant began notifying them of the Data Breach.

26. Defendant has been vague on its response to the Data Breach, telling announcing that it "moved quickly to investigate and respond to this incident, assess the security of its systems, and notify potentially affected individuals. In response to this incident, IGG augmented its policies and procedures addressing network security. IGG accelerated the implementation of an enhanced managed Security Operations Center including the deployment of an endpoint detection and response platform in response to this event with policies enabled specially for ransomware. IGG immediately reset passwords and employees with privileged access to sensitive systems were enrolled into our multifactor authentication platform."[5]

27. As of this writing, Defendant has offered no concrete information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

28. Appallingly, Defendant is offering no additional assistance to Plaintiff and class members beyond the entirely inadequate monitoring suggestions that are a part of its notice.

---

[5] *Id.*

29. This response is entirely inadequate to Plaintiff and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

30. In particular, Plaintiff was notified on or around March 1, 2022 by the Internal Revenue Service that a fraudulent tax return was filed in his name.

31. Plaintiff now faces significant delays in receiving his 2021 tax refund, as well as having spent and needing to spend significant time and effort to ensure that the IRS recognizes his actual tax return and needing to ensure that in the future, this does not happen again. This will require efforts on his part for years to come, if not the rest of his life.

32. Plaintiff is not aware of any other data breaches that could have resulted in the theft of his Social Security number. He is very careful about sharing his SPI, and has never knowingly transmitted unencrypted SPI over the internet or any other unsecured source.

33. Additionally, the Data Breach provided all the information necessary for a criminal to file a fraudulent tax return in Plaintiff's name.

34. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

35. Plaintiff and Class members provided their SPI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the cellular communications services industry preceding the date of the breach.

37. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

38. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[6] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[7]

39. The SPI of Plaintiff and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, driver license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

---

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, (last accessed April 30, 2022)

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

41. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

42. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

43. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

44. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

45. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

48. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

49. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

50. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

51. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

52. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

53. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8]

54. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[9]

55. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

56. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last accessed April 30, 2022).

[9] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 30, 2022).

into the new Social Security number."[10]

57. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[11]

58. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

59. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

60. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional

---

[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed April 30, 2022)

[11] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 30, 2022)

Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

61. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

62. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

63. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

64. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number,

---

[12] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last accessed April 30, 2022)

name, and date of birth.

65. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[13]

66. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits."[14]

67. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about April 23, 2022 (the "Nationwide

---

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed April 30, 2022)

[14] https://www.identityguard.com/news/kids-targeted-identity-theft (last accessed April 30, 2022)

Class").

69. The California Subclass is defined as follows:

All natural persons residing in California whose SPI was compromised in the Data Breach announced by Defendants on or about April 23, 2022 (the "California Subclass").

70. The California Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

71. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

72. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

73. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has not indicated the number of affected individuals as of this writing, but Plaintiff is informed and so believes that the number is in the thousands, if not higher. The Classes are readily identifiable within Defendant's records.

74. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable

measures to keep the SPI of Plaintiff and members of the Classes secure and to prevent loss or misuse of that SPI;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI had been compromised;

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL");

l. Whether Defendant violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA"); and

m. Whether Defendant violated California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA").

75. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

76. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

77. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action

will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

78. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the California Subclass as a whole.

79. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Breach of Implied Contract
(By Plaintiff Individually and on Behalf of the Nationwide Class)

80. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

81. When Plaintiff and Class Members provided their SPI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

82. Defendant solicited and invited Plaintiff and Class Members to provide their SPI as part of Defendant's regular business practices and as essential to the services transactions entered into between Defendant on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendant on the other hand. Plaintiff and Class Members accepted Defendant's offers by providing their SPI to Defendant in connection with their purchases from Defendant.

83. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

84. Defendant's implied promise to safeguard Plaintiff's and Class Members' SPI is evidenced by a duty to protect and safeguard SPI that Defendant required Plaintiff and Class Members to provide as a condition of entering into consumer transactions with Defendant.

85. Plaintiff and Class Members paid money to Defendant to purchase services from Defendant. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the purchases to obtain adequate data security. Defendant failed to do so.

86. Plaintiff and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from patients' continued use of Defendant's services—that Defendant would adequately safeguard SPI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

87. Plaintiff and Class Members value data security and would not have provided their SPI to Defendant in the absence of Defendant's implied promise to keep the SPI reasonably secure.

88. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

89. Defendant breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

90. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

91. Plaintiff and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

92. Plaintiff and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Nationwide Class members.

SECOND CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unlawful Business Practices
(By Plaintiff Individually and on Behalf of the California Subclass)

93. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

94. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Subclass.

95. Defendant engaged in unlawful acts and practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' SPI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' SPI in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security procedures and practices to safeguard the SPI of Plaintiff and the Nationwide Class and California

Subclass members. Defendant also violated: the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. and the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., as alleged below; and also the California Financial Information Privacy Act, California Financial Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

96. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the data breach to California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

97. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

98. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass members' SPI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

99. California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and California Subclass members of money or property that Defendants may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

THIRD CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unfair Business Practices
(By Plaintiff Individually and on Behalf of the California Subclass)

100. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

101. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' SPI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' SPI in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff's and California Subclass members. They were likely to deceive the public into believing their SPI was securely stored when it was not. The harm these practices caused to Plaintiff and the California Subclass members outweighed their utility, if any.

102. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Subclass members' SPI from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass members. They were likely to deceive the public into believing their SPI was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Subclass members outweighed their utility, if any.

103. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide Class and California Subclass members' legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

104. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass members' SPI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-

named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclasses.

105. Plaintiff and California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the California Subclass members of money or property that the Defendant may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

FOURTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(By Plaintiff Individually and on Behalf of the California Subclass)

106. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

107. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Subclass members' nonencrypted and nonredacted SPI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the SPI of Plaintiff and California Subclass members.

108. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass members' SPI was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems and/or from the dark web, where hackers further disclosed Defendant's customers', employees', former employees' and their dependents' SPI.

109. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass members' legally protected

interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

110. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass members' SPI and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass members.

111. Defendant is a limited liability company that is organized or operated for the profit or financial benefit of its shareholders, with a reported revenue of $37 million a year.[15] Defendant collects consumers' SPI as defined in Cal. Civ. Code § 1798.140.

112. At this time, Plaintiff and California Subclass members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs, and any other relief the court deems proper.

113. Concurrently with the filing of this complaint, Plaintiff provided written notice to Defendant identifying the specific provisions of this title he alleges they have violated. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff intends to amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

FIFTH CLAIM FOR RELIEF
Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*
(By Plaintiff Individually and On Behalf of the California Subclass)

114. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

---

[15] https://www.zoominfo.com/c/illinois-gastroenterology-group-llc/358267872 (last accessed April 30, 2022)

115. The California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. ("CLRA"), was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendant's acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendant's medical services are intended to and did result in sales of medical services.

116. Plaintiff and the other California Subclass members are consumers within the meaning of Cal. Civ. Code §1761(d).

117. Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network and deceptively representing that it adequately maintained such information, Defendant violated the CLRA. Defendant had exclusive knowledge of undisclosed material facts, namely, that its network was defective and/or unsecure, and withheld that knowledge from California Subclass members.

118. Defendant's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.
>
> For purposes of the CLRA, omissions are actionable along with representations.

119. Defendant stored California Subclass members' SPI on its network. Defendant represented to California Subclass members that its network was secure and that its SPI would remain private.

120. Defendant knew or should have known that it did not employ reasonable measures that would have kept California Subclass members' SPI secure and prevented the loss or misuse of their SPI. For example, Defendant failed to take reasonable steps to prevent the loss of SPI through its servers through appropriate encryption and industry best practices.

121. Defendant's deceptive acts and business practices induced California Subclass members to provide SPI, including Social Security numbers and driver's license numbers, for the purchase of insurance services. But for these deceptive acts and business practices, California Subclass members would not have purchased insurance services, or would not have paid the prices they paid for the insurance services.

122. Defendant's representations that it would secure and protect California Subclass members' SPI in their possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase insurance services.

123. California Subclass members were harmed as the result of Defendant's violations of the CLRA, because their SPI was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their SPI; and their SPI was disclosed to third parties without their consent.

124. California Subclass members suffered injury in fact and lost money or property as the result of Defendant's failure to secure their SPI; the value of their SPI was diminished as the result of Defendant's failure to secure their SPI; and they have expended time and money to rectify or guard against further misuse of their SPI.

125. Defendant's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

126. As the result of Defendant's violations of the CLRA, Plaintiff, on behalf of himself, California Subclass members, and the general public of the State of California, seeks injunctive relief prohibiting Defendant from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendant's conduct violated the CLRA.

127. Pursuant to Cal. Civ. Code § 1782, concurrently with the filing of this complaint, Plaintiff mailed Defendants notice in writing, via FedEx, of its particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendant's legal obligations, and to give notice to all affected customers of their intent to do so. If Defendant fails to respond to the letter within 30 days and to take the actions demanded to rectify their violations of the CLRA, Plaintiff will amend this complaint to seek damages and attorneys' fees as allowed by the CLRA.

SIXTH CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Nationwide Class)

128. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 79.

129. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

130. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

131. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

132. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

133. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

134. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' SPI;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and

Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and postjudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: May 2, 2022

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*
Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Putative Class